

Surat Buat Presiden

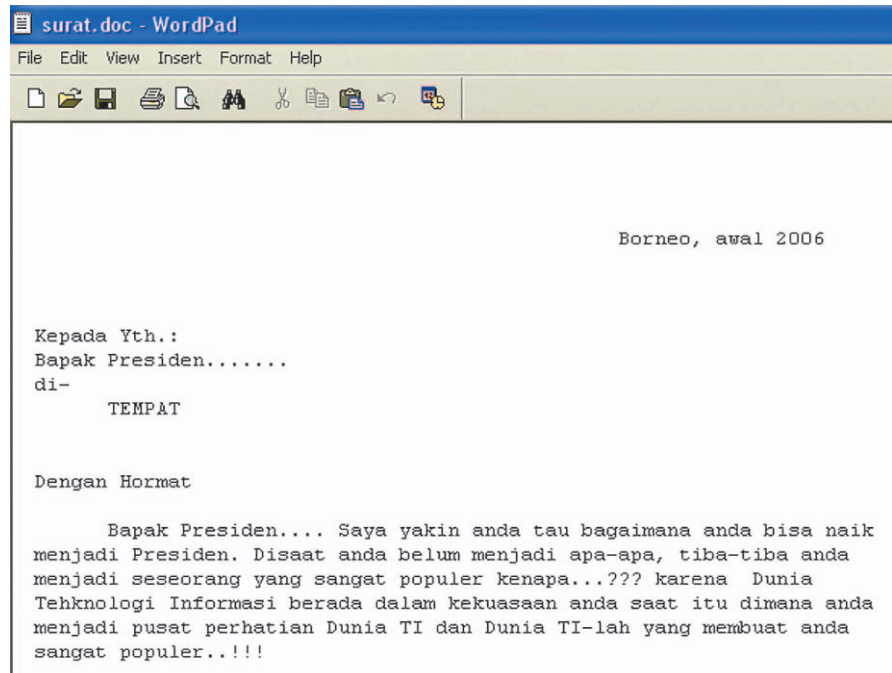
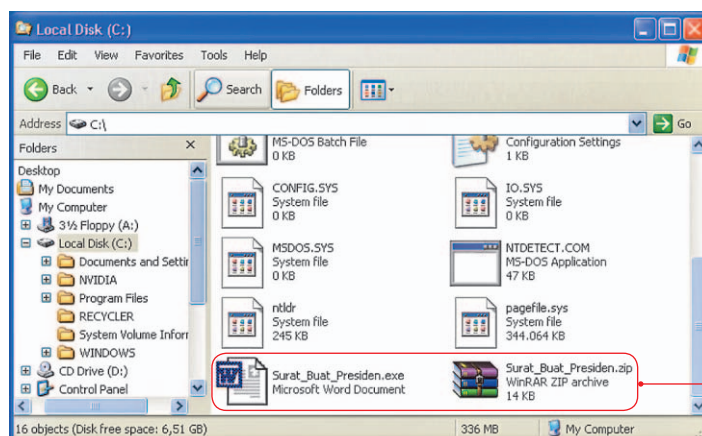
Seperti tidak kekurangan ide, para pembuat virus atau *virus maker* lokal, selalu saja bisa membuat korbannya tertipu. Kini hanya dengan iming-iming berupa file yang berisikan pesan yang dibuat oleh sang empunya virus, tidak sedikit korban yang tertipu.

Arief Prabowo

Surat yang dimaksud adalah surat yang skatanya *sih* ditujukan untuk Bapak Presiden. Virus yang dikenal juga dengan nama Borneo ini dapat menyebar melalui removable disk, e-mail, dan jaringan. Tingkat penyebaran virus ini cukup cepat, karena banyak juga pengguna komputer yang melaporkan bahwa komputernya terinfeksi oleh ulah si Borneo.

Virus Borneo atau Surat Buat Presiden juga oleh beberapa antivirus lain dikenal sebagai Trojan Backdoor.Win32.IRCBot. Mengapa? Karena virus ini juga memanfaatkan *script* IRC (*Internet Relay Chat*) untuk penyebarannya.

Virus Borneo yang terdapat pada root drive.



Penggalan surat dari Borneo.

Borneo ini dibuat menggunakan bahasa C++. Pada sampel yang kami punya virus ini tidak di-compress dan memiliki ukuran file sebesar 32.768 bytes. Virus ini juga akan mencoba untuk menghapus file-file Microsoft Word Anda, dan menggantinya dengan tubuh virus dengan nama file sama seperti dokumen yang Anda punya, hanya

extension-nya berformat *executable*, jadi berhati-hatilah.

Virus yang didesain agar dapat terlihat seperti file dokumen Microsoft Word ini, menggunakan icon MsWord sebagai icon utama dari program virus. Lalu pada *Version Information*, informasinya dibuat sedemikian mungkin agar menyerupai file dokumen Microsoft Word, ini bisa Anda lihat dengan mengklik kanan file *virus>Properties>Version*.

Bagaimana Ia Menginfeksi?

Pada saat menyerang komputer ia akan mencoba untuk meregister dirinya sebagai *service*, dengan cara meng-overwrite service dari System Restore dan digantikan dengan dirinya sendiri. Ia juga akan memeriksa pada harddisk komputer korban apakah terdapat direktori Microsoft Office (biasanya direktori MsOffice ini terdapat di "C:\Program Files\Microsoft Office\Office"). Apabila tidak ada, virus ini akan membuat direktorinya dan meng-copy-kan dirinya sendiri ke direktori tersebut dengan nama file "MSOHEV.EXE". Lalu ia akan membuat sebuah file *shortcut* pada StartUp folder untuk All Users dengan

| REGISTRY ITEM | INFORMATION |
|---|--|
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SafeBoot\AlternateShell | Virus mengubah value dari AlternateShell agar dapat berjalan di safe-mode. |
| HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell | |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\lsrvice\ImagePath | Mengubah value dari ImagePath yang asli agar virus ini dapat berjalan otomatis saat start Windows sebagai service. |
| HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lsrvice\ImagePathService | |

Tabel1. Beberapa item registry yang dirubah agar virus dapat tetap exist di komputer korbannya.

nama "Microsoft Office.Ink" yang diarahkan pada file virus yang telah ia copy-kan sebelumnya di direktori MsOffice tadi.

Direktori Windows juga dipercaya untuk menyimpan file induk dan file pendukung virus ini, di antaranya "Surat.doc" yang merupakan file teks yang berisi pesan sang empunya virus, Database.txt, Documents.exe, dan beberapa file executable yang merupakan file induk virus seperti "SVCHOST.exe", "SVCHOST.exe", dan "Winlogon.exe". Terlihat pada file induk virus, ia menyamaran dengan mengganti huruf "O" dengan angka "0" agar sekilas terlihat sama seperti file SVCHOST.EXE dan WINLOGON.EXE yang dimiliki oleh Windows. Lalu dengan menggunakan program internal Windows yakni attrib, ia menjalankan perintah "attrib +r +h +s %namafile%" untuk mengeset atribut file induk sebagai file Read Only + Hidden + System.

Virus juga akan mencoba meng-copy-kan dirinya sendiri ke setiap root drive yang ditemukannya dengan nama "Surat_Buat_Presiden.exe" dan memeriksa apakah pada komputer korban juga terdapat program kompresi, seperti WinRAR ataupun WinZIP. Apabila ada, dengan bantuan aplikasi tersebut ia akan meng-compress dirinya sendiri dan ditaruhnya juga di root drive dengan nama "Surat_Buat_Presiden.zip".

Aksinya tidak sampai di situ saja, apabila komputer korban tersebut terhubung ke jaringan, ia juga akan melakukan searching pada jaringan tersebut dengan range IP 192.168.x.x. Apabila sharing folder yang ditemukan dapat diakses dan mempunyai hak akses write, ia akan meng-copy-kan file seperti apa yang telah ia buat sebelumnya pada root drive.

Untuk penemuan filenya memang ia buat semenarik mungkin agar orang tergoda untuk membuka file tersebut. Lagi-lagi ini masalah social engineering yang selalu memenangkan pertempuran antara virus dan sang user. Seperti yang diutarakan di awal, virus ini juga akan mencoba untuk mengirimkan dirinya melalui e-mail menggunakan MAPI (Mail Application Programming Interface).

Manipulasi Registry

Seperti virus-virus yang lain, Borneo juga akan mengubah beberapa item registry. Salah satunya adalah dengan mengubah registry agar virus ini dapat berjalan pada modus safe-mode sekalipun.

Lalu seperti yang diutarakan diawal, dengan bantuan registry juga, virus ini mengubah setting-an untuk service System Restore milik Windows. Yakni, dengan mengubah value dari ImagePath, tempat menyimpan alamat file service System Restore agar diarahkan ke file virus. Inilah yang menyebabkan sang virus akan selalu aktif setiap kali menjalankan Windows. Tapi, tidak seperti virus lainnya, virus ini tidak men-disable tools atau fungsi Windows seperti Task Manager, Registry Editor, MsConfig, ataupun Folder Options seperti kebanyakan virus lokal lainnya.

Aktif di Memory

Pada komputer yang terinfeksi, apabila kita buka Task Manager dan dilihat secara sekilas tidak ada nama-nama process yang mencurigakan. Inilah seperti yang dikatakan tadi bahwa nama file induk virus ini dibuat semirip mungkin dengan file process/service milik Windows, yakni SVCHOST.exe ataupun

WINLOGON.exe. Hanya saja, ia mengganti huruf O nya dengan angka 0 sehingga sekilas akan terlihat sama.

Saat aktif di memory, virus ini memiliki beberapa process induk yang saling terkait, yakni "Winlogon.exe", "SVCHOST.exe" atau "SVCHOST.exe". Jadi dalam membuatnya, sang programmer virus tersebut membuat semacam fungsi timer atau dengan fungsi looping sehingga virusnya dapat secara terus menerus memonitor keberadaannya di memory satu sama lain.

Lalu apa yang terjadi apabila kita mengkill salah satu process tersebut? Apabila itu terjadi, maka virus akan mencoba untuk mendapatkan akses shutdown/restart dengan mengeset access privilege untuk SeShutdownPrivilege. Apabila berhasil maka ia akan me-restart Windows Anda. Ini dilakukannya agar mempersulit program antivirus ataupun si user sendiri dalam menghapus virus tersebut.

Kami telah meng-update PCMAV agar dapat membasmi virus ini. Untuk penggunaan PCMAV secara optimal, apabila pada komputer Anda terdapat program antivirus lain, matikan dulu fasilitas real time protection-nya. Apabila komputer Anda terinfeksi, silakan scan menggunakan PCMAV RC6 ini. Namun apabila ternyata PCMAV tidak bisa mendeteksi virus Borneo yang menyerang komputer Anda, silakan Anda kirimkan sampelnya kepada kami. Kami tunggu! ■

The screenshot shows the Process Explorer window from Sysinternals. The main window lists several processes, with 'explorer.exe', 'WINLOGON.exe', and 'SVCHOST.exe' highlighted in a red box. A red arrow points from this box to a smaller inset window below, which shows a detailed view of these processes. The inset window lists the process name, PID, CPU usage, and description for each.

| Process | PID | CPU | Description |
|--------------|------|-----|---------------------|
| explorer.exe | 1360 | 9 | Windows Explorer |
| WINLOGON.exe | 2024 | 1 | Microsoft Word D... |
| SVCHOST.exe | 2036 | 2 | Microsoft Word D... |

Virus Borneo yang telah aktif di memory.